Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1440 10/12/12

~ Policing Social Media! ~ People Are Talking! ~ Huawei, Spy Opening?
~ Virus Targets Venezuela ~ Assange Is A Sellout? ~ New Facebook Buttons!
~ Wow Hacked w/ Corpses! ~ Death Threats Malware! ~ Smaller iPad Soon!

~ ThisLife Photo Storage! ~ Tempting As Butts, Sex ~ Ballmer’s Bonus Cut!

-* US Warns of Iran Cyberattack *-
-* Philipines Suspends Cybercrime Law! *-
-* Maine Republican Blasts Opponent Over WoW! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

I didn’t see or listen in to the VP debate, but I did "see" a portion of it after work the other night. Didn’t hear it, but was looking at the TV while doing something else. All I could see was Biden grinning and laughing at some of Ryan’s comments - how arrogant he appeared in doing so. I was never a big Biden fan, and these displays only reaffirmed my lack of respect for the man. From what I saw, Biden did nothing to overcome the President’s poor showing during the first debate. Never a dull moment!

Autumn has certainly taken a firm grip on New England. The weather has turned a lot more cool lately, and the leaves have started to turn here in the southern portion of the region. Time to get ready to start cleaning up the aftermath of the leaves falling!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Hack Fills ’World of Warcraft’ Cities With Corpses!
""""""""""""""""""""""""""""""""" Maine GOP Blast Opponent for WoW Play!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Hack Fills ’World of Warcraft’ Cities With Corpses

An exploit in World of Warcraft allowed hackers to kill thousands of characters in the game’s major cities over the weekend.

YouTube videos and screenshots surfaced of thousands of players and non-player characters dying in the populated towns of Stormwind and Orgrimmar Sunday morning.

According to Eurogamer, the hacker posted that they had found "a kill hack" that allowed level 1 characters to bring down everyone around them without even attacking.

"We didn’t do any permanent damage. Some people liked it for a new topic of conversation and a funny stream to watch, and some people didn’t. The people who didn’t should be blaming Blizzard for not fixing it faster (four hours of obvious use is sad)," Eurogamer reports the unknown hacker said. "It’s not like I added 20,000,000 gold to everyone’s inventory and broke the economy, but look at the big Chinese gold seller companies who are doing this every day. Now ask yourself who is really ruining the game. It’s not. That’s my justification."

Blizzard community manager Nethaera said on the World of Warcraft community forums that the exploit had been "hotfixed" and "should not be repeatable."

The newest World of Warcraft expansion came out two weeks ago, and the popular massively multiplayer game still has about 10 million subscribers worldwide. Nethaera urged players to keep playing, saying, "It’s safe to continue playing and adventuring in major cities and elsewhere in Azeroth."

Maine Republicans Blast Opponent for World of Warcraft Play

A Maine Senate race has turned into a fight over trolls, dwarves and goblin-like creatures known as orcs.

In a mailing this week, state Republicans accused Democrat Colleen Lachowicz of living in a fantasy world and making "crude, vicious and violent comments" in online forums dedicated to World of Warcraft, a popular online game.

Lachowicz, who is challenging incumbent Senator Tom Martin, has responded by accusing Republicans of focusing on her hobbies rather than public policy issues.

"I think it’s weird that I’m being targeted for playing online games," she said in a statement. "What’s next? Will I be ostracized for playing Angry Birds or Words With Friends?"

A website produced by Republicans includes a link to Lachowicz’s online character, Santiaga, who sports a purple Mohawk and is armed with a meteor shard. It notes that the game takes place in a "make believe land Azeroth" and that Lachowicz is "playing at level 85 the highest level one can attain."

The mailing said she spends hundreds of hours involved in World of Warcraft, which features an array of characters such as trolls and orcs.

"We need a senator who lives in our world, not Colleen’s world," the mailing said.

It also highlights comments Lachowicz made in online forums to other World of Warcraft players in 2009 and 2010, including: "I love poisoning and stabbing," "I can kill stuff without going to jail" and "I like to stab things and I'm originally from New Jersey, what's your (expletive) point?"

Ericka Dodge, a spokeswoman for Maine Democrats, said in an interview on Friday that Lachowicz, a social worker, had only spent about 30 minutes playing World of Warcraft since January as she was now spending her free time campaigning.

"Clearly before she started the campaign she spent a lot more time gaming," said Dodge. "She's also a knitter, but my guess is no one is going to attack her for that."

An estimated 211.5 million people, or about two-thirds of the population, play video games in the U.S., according to NPD Group.

David Sorensen, a spokesman for the Maine Republican Party, said the mailing and website weren't meant to antagonize gamers.

"As far as we're concerned, it's not a World of Warcraft story,' it's a candidate saying outrageous things through World of Warcraft story,'" he said on Friday.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Philippine Supreme Court Suspends Cybercrime Law

The Philippine Supreme Court on Tuesday suspended implementation of the country's anti-cybercrime law while it decides whether certain provisions violate civil liberties.

Justice Secretary Leila de Lima said the court issued a temporary restraining order stopping the government from enforcing the law signed by President Benigno Aquino III last month. The law took effect last week but there has been no report of anyone being charged with violating it.

The court suspended the law for 120 days and scheduled oral arguments for Jan. 15. It ordered the government to respond within 10 days to 15 petitions seeking to declare the law unconstitutional.

The law aims to combat Internet crimes such as hacking, identity theft, spamming, cybersex and online child pornography.

Journalists and rights groups oppose the law because it also makes online libel a crime, with double the normal penalty, and because it blocks access to websites deemed to violate the law. They fear such provisions will be used by politicians to silence critics, and say the law also

violates freedom of expression and due process.

Brad Adams, Asia director for Human Rights Watch, commended the court and urged it to "go further by striking down this seriously flawed law."

In one of the petitions filed with the court questioning the law's constitutionality, the National Union of Journalists of the Philippines said it would "set back decades of struggle against the darkness of 'constitutional dictatorship' and replace it with 'cyber authoritarianism.'"

Many Facebook and Twitter users and the portals of media organizations in the Philippines have replaced their profile pictures with black screens to protest the law. Hackers also defaced several government websites in protest.

Renato Reyes, secretary general of the left-wing New Patriotic Alliance, another petitioner, said the court's order was "a major victory for freedom and civil liberties."

Aquino has supported the online libel provision, saying people should be held responsible for their statements. But he has also said he is open to lowering the penalties.

Several legislators, including some who approved the law, have said they will try to amend the law to address civil-rights concerns.

US Warning Reflects Fears of Iranian Cyberattack

Defense Secretary Leon Panetta's pointed warning that the U.S. will strike back against a cyberattack underscores the Obama administration's growing concern that Iran could be the first country to unleash cyberterrorism on America.

Panetta's unusually strong comments Thursday came as former U.S. government officials and cybersecurity experts said the U.S. believes Iranian-based hackers were responsible for cyberattacks that devastated computer systems of Persian Gulf oil and gas companies.

Unencumbered by diplomatic or economic ties that restrain other nations from direct conflict with the U.S., Iran is an unpredictable foe that national security experts contend is not only capable but willing to use a sophisticated computer-based attack.

Panetta made it clear that the military is ready to retaliate though he didn't say how if it believes the nation is threatened by a cyberattack, and he made it evident that the U.S. would consider a preemptive strike.

"Iran is a country for whom terror has simply been another tool in their foreign policy toolbox, and they are a country that feels it has less and less to lose by breaking the norms of the rest of the world," said Stewart Baker, former assistant secretary at the Department of Homeland Security and now in private law practice. "If anybody is going to release irresponsible unlimited attacks, you'd expect it to be Iran."

National security experts have long complained that the administration needs to be much more open about what the military could and would do if

the U.S. were to be the victim of cyberattacks. They argue that such deterrence worked in the Cold War with Russia and would help convince would-be attackers that an assault on America would have dire results.

Panetta took the first steps toward answering those critics in a speech analysts said was a thinly veiled warning to Iran, and the opening salvo in the campaign to convince Tehran that any cyberattack against America would trigger a swift and deadly response.

"Potential aggressors should be aware that the United States has the capacity to locate them and hold them accountable for actions that harm America or its interests," Panetta said in a speech in New York City to the Business Executives for National Security.

And while he did not directly connect Iran to the Gulf cyberattacks, he warned that Iran's abilities were growing.

Security analysts agree.

The presumed Iranian cyberattacks hit the Saudi Arabian state oil company Aramco and Qatari natural gas producer RasGas using a virus, known as Shamoon, which can spread through networked computers and ultimately wipes out files by overwriting them.

In his speech, Panetta said the Shamoon virus replaced crucial system files at Aramco with the image of a burning U.S. flag, and also overwrote all data, rendering more than 30,000 computers useless and forcing them to be replaced. He said the Qatar attack was similar.

"This one worries me," said Richard Bejtlich, chief security officer for the Virginia-based cybersecurity firm Mandiant. "I'm not an alarmist, but when I saw that 30,000 computers at Saudi Aramco got just deleted, that was a big deal. You don't see the Chinese government, you don't see the Russian government, or even their patriotic hackers go out and delete anything for the most part."

From the Iranians' point of view, however, attacks against the U.S. may be justified because American sanctions leveled on the country for refusing to cooperate with international norms on its nuclear program have hit Iran hard. Tehran also believes that the U.S. and Israel were behind the Stuxnet cyberattack that forced the temporary shutdown of thousands of centrifuges at a nuclear facility there in 2010.

As a result, said Bejtlich, Iran already believes it is at war with the U.S.

Frank Cilluffo, , a former special assistant for homeland security to President George W. Bush, said U.S. authorities have suspected Iran of trying to plot cyberattacks against American targets, including nuclear plants. And he said that Iran's Revolutionary Guard Corps appears to now be trying to bring some of the patriotic hacker groups under its control, so it can draw on their abilities.

"Iran has been doing a lot of cyber saber-rattling," said Cilluffo, now director of George Washington University's Homeland Security Policy Institute. "What they lack in capabilities, they more than make up for in intent."

Tehran has not made any public comment on Panetta's comments, but the Iranians routinely report the discovery of viruses and other malicious

programs in government, nuclear, oil and industrial networks, blaming Israel and the United States.

While Panetta's warnings received high marks from security experts, those people also were quick to say that much more needs to be done.

The U.S., said former Homeland Security Secretary Michael Chertoff, must lay out the rules of the road and figure out what kind of proof authorities would need before taking action.

"We still have work to do," said Chertoff, who is now chairman of the Chertoff Group, a global security firm. "Will we take action to preempt something rather than simply retaliate, and how early and how much warning will we need before we take that action?"

He noted that most conflicts arise over misunderstandings, when one side doesn't realize what the other will do if provoked.

The administration has repeatedly warned of the cybersecurity threats, particularly against critical infrastructure such as financial networks, transportation systems and utility companies. More recently, the White House has been considering using the president's executive power to encourage critical industries to better protect their networks because legislation to do so stalled in Congress.

"While the message has been sent over and over again it doesn't seem to have acquired urgency across the board," said Chertoff. "We need to make it clear that this is not just background noise you have to deal with, but that it really strikes at the fundamentals of our national security."

New Computer Virus Targets Venezuelans After Vote

A newly detected computer virus aims to steal Venezuelans' online credentials using a link that purports to reveal information about the country's recent presidential election, the digital security company Kaspersky Lab said on Friday.

The malicious software was launched after Venezuela's Oct. 7 presidential election and was spread by email, said Dmitry Bestuzhev, head of the Moscow-based company's research and analysis team in Latin America.

At least 75 Kaspersky customers came under attack by the malware, and non-customers surely did, too, he said.

Bestuzhev said in a blog post on Friday that the malicious file is named "listas-fraude-electoral.pdf.exe," which translates as "electoral fraud lists" a title likely to make some Venezuelans curious after President Hugo Chavez's re-election victory.

He explained by email that computer users received an email message with a link. Once a victim clicked on the link, he said, the person was redirected to a fake website purporting to belong to the Venezuelan television channel Globovision.

"After the click the malicious file was automatically downloaded," Bestuzhev said. However, Kaspersky Lab said its antivirus system successfully blocked each attempt by the malware to infect its customers'

computers.

Bestuzhev said the malware allows criminals to steal victims' banking information and also online credentials for those holding accounts with Venezuela's currency agency, known by its Spanish initials CADIVI.

Venezuela's government maintains strict foreign currency exchange controls, and the currency agency provides people who apply with limited amounts of dollars or other currencies for purposes including travel, certain imported goods and overseas tuition payments.

The malware was designed to gain access to Venezuelans' CADIVI accounts to use their allotted dollars, Bestuzhev said.

"Being that this malware is quite simple and also targeting only Venezuelan banks and CADIVI, we can strongly assume that the cybercriminals who produced it are from Venezuela too," he wrote on the blog.

Officials at the government's currency agency and Science and Technology Ministry could not be immediately reached for comment.

Bestuzhev said the malware was detected by was "proactive crawlers," which work like a sort of search engine and are designed to hunt down malicious URLs.

Huawei, ZTE Provide Opening for China Spying

Huawei Technologies Co. and ZTE Corp., China s two largest phone-equipment makers, provide opportunities for Chinese intelligence services to tamper with U.S. telecommunications networks for spying, according to a congressional report released today.

The House intelligence committee report said the companies failed to cooperate with a yearlong investigation and to adequately explain their U.S. business interests and relationship with the Chinese government.

Huawei and ZTE seek to expand in the United States, but as a result of our investigation, we do not have the confidence that these two companies with their ties to the Chinese government can be trusted with infrastructure of such critical importance, the committee s chairman, Michigan Republican Mike Rogers, said.

The U.S. government should block acquisitions or mergers by Huawei and ZTE, the report said. Government agencies and contractors shouldn t use equipment from the companies, and U.S. intelligence agencies should remain vigilant and focused on this threat, the report recommended.

The House investigation found credible reports of illegal behavior by Huawei, including immigration violations, bribery and corruption, based on statements from current and former employees, according to the report. Allegations will be referred to federal agencies including the Homeland Security and the Justice departments, according to the report, which didn t provide full details or identify the accusers.

The committee will forward information on a clear case of bribery in order to get a contract here in the United States to the Federal Bureau

of Investigation, probably tomorrow, Rogers said at a U.S. Capitol news conference today with the panel s top Democrat, Maryland Representative C.A. Dutch Ruppersberger.

Huawei, in a statement today, said the report employs many rumors and speculations to prove non-existent accusations. The committee pre-determined the outcome of its investigation, the company said.

The quality, the integrity of our products are world proven, William Plummer, a Washington-based spokesman for the company, said in an interview after the committee members spoke. It is a political distraction, it is a dangerous thing, to suggest that you can solve these vulnerabilities by embargoing a company. It s a false sense of security. It ignores the fact that this is a global industry.

Dai Shu, a ZTE spokesman, called it noteworthy that after a yearlong investigation, the committee rests its conclusions on a finding that ZTE may not be free of state influence. That standard would apply to any company operating in China, Dai said in an e-mailed statement.

Almost all telecommunications-infrastructure equipment sold in the U.S., by any company, contains Chinese-made components, Dai said. ZTE recommends that the committee s investigation be extended to include every company making equipment in China, including Western companies that use equipment made by Chinese joint-venture partners and suppliers, Dai said.

Rogers and Ruppersberger announced the probe of the Chinese companies last November, citing concerns about hacking into U.S. systems and theft of intellectual property. U.S. counterintelligence officials called China the world s biggest perpetrator of economic espionage in a report last year, saying the theft of sensitive data is accelerating and jeopardizing an estimated $398 billion in U.S. research spending.

Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services, the report says.

The committee received reports that routing equipment supplied by Huawei to U.S. customers acted oddly, Rogers said. He cited a process known as beaconing, which he said involves unauthorized processing and sending of information. One example would be a router that turns on in the middle of the night and sends large packets of data to China, he said.

Huawei first learned of the beaconing allegation at a House intelligence committee hearing last month, and it s unclear what the committee is referring to, Plummer said in an interview.

New Malware Sends Your Friends Death Threats Through Your Email Aaccount

If your sweet old grandmother sends you an email threatening to slit your throat, don t worry: It s just the malware talking. NBC s TechNewsDaily reports that there s a new strain of malware going around in Japan that takes control of users email accounts and uses them to send out death threats to a variety of targets. In fact, the malware is apparently so convincing that three people in Japan so far have been arrested because their email accounts have sent out death threats they didn t write.

Among other things, Japanese authorities have seen the malware send out an email that threatened to kill en masse at a shopping center, an email sent to an airline that threatened to bomb a plane and an email sent to a school attended by a member of the Japanese royal family that threatened harm against the kindergarten class.

While this is all horrible, Symantec says that the malware s infection appears to be very limited at this time and the broader population of Internet users should be not affected. Symantec also says that its own Insight reputation-screening software was capable of protecting its users from the malicious code.

Anonymous Blows Off WikiLeaks, Calls Assange A Sellout

You ve changed, Wikileaks. You used to just be about the hacking! That s basically the message that hacker collective Anonymous delivered to WikiLeaks this week, as Anonymous sought to distance itself from Julian Assange s website in a statement posted on its Twitter account. As The Guardian reports, Anonymous described WikiLeaks as the one man Julian Assange show after the website began asking users to pay for access to millions of leaked documents. The group went on to decry Assange s current celebrity status antithetical to WikiLeaks original purpose.

The idea behind WikiLeaks was to provide the public with information that would otherwise be kept secret by industries and governments, the group said. But this has been pushed more and more into the background, instead we only hear about Julian Assange, like he had dinner last night with Lady Gaga. That s great for him but not much of our interest. We are more interested in transparent governments and bringing out documents and information they want to hide from the public.

Britain To Issue Guidelines on Policing Social Media

The Crown Prosecution Service (CPS) is holding discussions on laws governing social media, with the aim of publishing guidelines by Christmas, after a flurry of cases concerning inflammatory Twitter and Facebook comments.

Police have expressed concern at the growing number of such cases they are being called on to investigate.

This week alone, two people have been sentenced for social media offences.

Teenager Matthew Woods was sentenced on Monday to 12 weeks in prison for offensive jokes on Facebook about missing Welsh five-year-old April Jones.

A day later Azhar Ahmed, 20, was given 240 hours of community service after writing "all soldiers should die and go to hell" on Facebook following the death of six British soldiers in Afghanistan.

The CPS has invited academics, media lawyers, bloggers and the police to participate in a month-long discussion.

A CPS spokeswoman said the talks were not primarily aimed at changing current law.

"At the moment the idea is to have clear, consistent guidelines across the prosecution of these cases within the existing law", she said.

The Guardian newspaper said the CPS was keen to ask whether social media companies should improve their site moderation.

The police, who have expressed concern over dealing with the growing wave of offences, welcomed the discussions.

"Many offensive comments are made every day on social media and guidance will assist the police to focus on the most serious matters", said Andy Trotter, spokesman for the Association of Chief Police Officers.

He added it was not only a matter of principle but "also the practicality of dealing with thousands of potential offences".

However, some say it is common sense rather than official guidelines that is needed for dealing with cases involving social media.

They include barrister John Cooper, who successfully defended a man in July who had been prosecuted for sending a "menacing" message threatening to blow up Doncaster’s Robin Hood airport. The court ruled that message had been a joke and dismissed the case.

"The guidelines tend to be so strict that it actually railroads people into prosecuting where normally they wouldn’t," he told Reuters.

The guidelines removed "discretion and the need and operation of common sense", Cooper added.

Facebook Experiments With ’Want’ and ’Collect’ Buttons

Do you like Facebook’s "Like" buttons? People use them for all sorts of reasons - there’s even an experiment in which you can click on it to send hugs - but Facebook, in the meantime, is experimenting with a few variations.

Facebook is testing new "want" and "collect" buttons for its new "Collections" feature. The new buttons, which only appear so far on a few select pages, allow users to create "wish lists" of the stuff they, well, wish for. The wish list is a gallery of sorts of all the items you’ve collected or wanted.

The feature is live now on such pages as Pottery Barn’s. I was able to hit the "collect" button there on a Hadley Ruched Duvet and add it to my "For the Home" wish list. Facebook is testing the Collections feature with Fab.com, Michael Kors, Victoria’s Secret, Wayfair.com, and others. If you are a fan of any of those retailers the collections might appear in your News Feed.

Collections is Facebook’s second experiment in the last two weeks as it tries out a move into the e-commerce space. Last week Facebook released Gifts, which allows you to buy items for friends directly through the

site.

With Collections you don’t actually buy the items on Facebook.com, but you do show your interest.

"Collections can be discovered in News Feed, and people will be able to engage with these collections and share things they are interested in with their friends. People can click through and buy these items off of Facebook," Facebook said in a statement.

There is a "buy" link directly under products you add to your wish lists, but Facebook told ABC News that it is not profiting directly from this feature and doesn’t have plans to. The new buttons won’t be available across the Web the way the Like button currently is either.

ThisLife Makes Online Photo Storage and Organization A Breeze

These days, many people upload their photos to numerous online services and it can sometimes be hard to keep track of them all. ThisLife, an app for iPhone and iPad, is a cloud solution for sharing and organizing your photos and videos. It allows you to import your photographs from web services like Flickr, Picasa, Facebook, Instagram and others, or you can simply upload the images from your computer.

As a company, ThisLife firmly believes that photographs should be treasured memories that need to be protected. This means understanding that organizing all your photos from disparate services isn t much fun. ThisLife automatically imports your photos, cleverly recognizes duplicates and faces, and even auto-enhances the images for the best image quality.

Its most interesting feature is how it creates a story of your images. It adds dates to each photo and it s easy to include a text or audio note to enhance this storytelling experience. At the same time, ThisLife makes it straightforward to browse and rearrange your photos any way you choose. You can create themed albums, and the app is also clever enough to retain social networking information such as Facebook likes.

Once you are done organizing your images, it s simple to share them via Facebook, Twitter, Tumblr or email. However, you can set your albums to private if you don t want others to see them. The interface is elegant and smooth, even with many photos stored, and the quality of them is impressive. It s encouraging to see ThisLife store the original images (even if it enhances them) and doesn t resize them so they lose quality.

The app is free, at least initially. You ll get the opportunity to store up to 1,000 images and 1 hour of videos with the basic Simple Plan. While that does sound like a lot, you ll be surprised how many photos you ve probably stored via various apps once ThisLife starts to dig around. Pay $7.99/month (or $79.99/year) for the Adventure Plan, and your storage is upped to 20,000 images and 10 hours of video at 1080p resolution. That should be enough for most people, but true photo and video fiends will appreciate the so-called Family Plan for $14.99/month (or $149.99/year) which offers 50,000 images and 25 hours of full HD video.

ThisLife is definitely worth a look, especially for free. The web service is effective, but it s really enhanced by the mobile experience. With

ThisLife, it s easy to show off your photos to people via your iPad or iPhone, and you re not losing precious storage space on your devices because photos are stored in the cloud instead.

Smaller iPad To Be Revealed October 23

Apple Inc. is set to reveal a smaller, cheaper version of the iPad at an event on Oct. 23, according to several reports published Friday.

The reports from Bloomberg News, Reuters and the AllThingsD blog are based on unnamed sources "familiar with the plans."

Apple Inc. hasn’t said anything about a smaller tablet, a concept company founder Steve Jobs derided two years ago. But company-watchers have assumed for months that an "iPad mini" will appear before the holiday season.

The screen is reportedly about half the size of the iPad’s, which measures 9.7 inches diagonally. Analysts speculate the starting price of the device could be about $299.

With the device, Apple could close an opening in the tablet market for rivals like Amazon.com Inc., whose Kindle Fire is half the size of the iPad and starts at $199. Google Inc. and Barnes and Noble Inc. also sell tablets in the same size and price range.

Apple’s event would occur three days before Microsoft Corp. releases Windows 8, the new version of its operating system. Microsoft will be releasing its "Surface" tablets with the software.

Microsoft Sets Windows 8 Price, Opens for Pre-order

Microsoft Corp opened its Windows 8 operating system for pre-orders on Friday, setting the price for an upgrade to the full version of the software at $70 for a DVD pack.

Users can also wait for launch on October 26 to download the system onto their computers for $40, an offer price that will expire at the end of January. PCs running Windows XP, Vista and Windows 7 will be able to upgrade to Windows 8.

Shoppers can reserve the software pack at Microsoft’s own stores, Amazon.com, Best Buy, Staples and elsewhere. Microsoft has not yet announced the price of the full software to install from scratch, as opposed to the upgrade. The current price for a comparable version of Windows 7 is $200.

Any customer who buys, or already bought, a Windows 7 PC between June 2 and the end of January 2013 will be able to get an upgrade to Windows 8 Pro for $15, a move designed to prevent a drop-off in PC sales before the launch of Windows 8.

Microsoft also said PC makers such as Acer, Asustek, Dell, HP, Samsung and Sony were also now taking pre-orders for machines with Windows 8

pre-installed.

The world’s largest software company did not mention its own Surface tablet PC, which is expected on the market at the same time as Windows 8. Microsoft has not revealed the price of the product it hopes will challenge Apple Inc’s iPad.

Facebook Is as Tempting as Cigarettes and Sex

How highly would you say you prioritize your Facebook-ing? A report by the University of Chicago Booth School of Business found that the desire to check social media platforms like Facebook, Twitter and Pinterest were among the toughest-to-resist temptations - equivalent to cigarettes and sex.

Subjects in the study, who were between ages 18 and 85, all living in Germany, were given BlackBerry devices and told to let the researchers know every 30 minutes if they felt a desire to drop by their social networks. They were also asked to document other impulses, like smoking, drinking and sleeping, among others, and rate them from "strong" to "irresistible." The temptation to visit social media platforms was more difficult to resist than the rest, researchers concluded.

Part of the reason for the surprising results, says lead author of the study Wilhem Hofmann, is social media’s high availability. After all, engaging in a tweet or Facebook post doesn’t take much effort - especially when you can do so with the touch of a few buttons.

Ballmer s Bonus Cut Due to Wilting Windows and Browser Blunders

If Steve Ballmer seems a little less frantic and energetic lately, there s a good reason for it: Microsoft missteps have cost him a healthy chunk of his bonus. According to Reuters, Microsoft s CEO saw his bonus cut by 9% year-over-year for flat sales of Windows and his failure to ensure that the company provided a choice of browser to some European customers. While no one should weep for Ballmer over losing money, this year s bonus cut is significant because it s the third consecutive year that he has failed to reach his maximum bonus, Reuters notes.

=~=~=~=